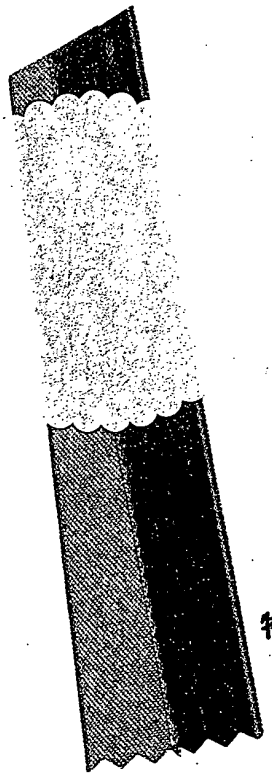
OFO14924
US/ma

# 日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

| | |
|---|---|
| 出願年月日<br>Date of Application: | ２０００年１０月２４日 |
| 出願番号<br>Application Number: | 特願２０００－３２３９８０ |
| 出願人<br>Applicant (s): | キヤノン株式会社 |

CERTIFIED COPY OF
PRIORITY DOCUMENT



２０００年１２月　８日

特許庁長官
Commissioner,
Patent Office　及川耕造

出証番号　出証特２０００－３１０２６７９

【書類名】　特許願

【整理番号】　4336003

【提出日】　平成12年10月24日

【あて先】　特許庁長官　殿

【国際特許分類】　H04N　1/00

H04L　9/00

【発明の名称】　通信装置及び方法並びに記憶媒体

【請求項の数】　20

【発明者】

【住所又は居所】　東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

【氏名】　佐藤　栄一

【特許出願人】

【識別番号】　000001007

【住所又は居所】　東京都大田区下丸子３丁目３０番２号

【氏名又は名称】　キヤノン株式会社

【代表者】　御手洗　冨士夫

【電話番号】　03-3758-2111

【代理人】

【識別番号】　100090538

【住所又は居所】　東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

【弁理士】

【氏名又は名称】　西山　恵三

【電話番号】　03-3758-2111

【選任した代理人】

【識別番号】　100096965

【住所又は居所】　東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

【弁理士】

【氏名又は名称】　内尾　裕一

【電話番号】　03-3758-2111

【先の出願に基づく優先権主張】

【出願番号】　平成11年特許願第325559号

【出願日】　平成11年11月16日

【手数料の表示】

【予納台帳番号】　011224

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9908388

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　通信装置及び方法並びに記憶媒体

【特許請求の範囲】

【請求項１】　第１のネットワークからの受信データを第2のネットワークへ転送する通信装置において、

前記受信データの転送先情報を判別する第１の判別手段と、

前記受信データの機密度情報を判別する第2の判別手段と、

前記第１および第2の判別結果に応じて、前記受信データの転送を実行する制御手段を有することを特徴とする通信装置。

【請求項２】　請求項１において、前記第１と第2の判別手段の少なくとも一方による判別に応じて、前記制御手段は前記受信データを暗号化して転送することを特徴とする通信装置。

【請求項３】　請求項１において、前記機密度情報は、前記受信データが親展データであるかどうかを含むことを特徴とする通信装置。

【請求項４】　請求項１において、前記第１と第2の判別手段の少なくとも一方による判別に応じて、前記制御手段は前記受信データを電子メールにより転送先に転送することを特徴とする通信装置。

【請求項５】　請求項１において、前記第１と第2の判別手段の少なくとも一方による判別に応じて、前記制御手段は前記受信データを所定のメモリに記憶することを特徴とする通信装置。

【請求項６】　請求項１において、前記転送先情報は、前記転送先に対応する暗号情報を具備しているかどうかを含むことを特徴とする通信装置。

【請求項７】　請求項１において、前記転送先情報は、前記受信データの転送先への経路情報を含むことを特徴とする通信装置。

【請求項８】　請求項１において、前記転送先情報は、前記転送先に対応する暗号情報が有効期限内にあるかどうかを含むことを特徴とする通信装置。

【請求項９】　第１のネットワークからの受信データを第2のネットワークへ転送する通信方法において、

前記受信データの転送先情報を判別する第１の判別工程と、



出証特２０００－３１０２６７９

前記受信データの機密度情報を判別する第2の判別工程と、

前記第１および第2の判別結果に応じて、前記受信データの転送を実行する制御工程を有することを特徴とする通信方法。

【請求項１０】　第１のネットワークからの受信データを第2のネットワークへ転送する通信方法のプログラムを格納したコンピュータ読取可能な記憶媒体において、

前記受信データの転送先情報を判別する第１の判別工程と、

前記受信データの機密度情報を判別する第2の判別工程と、

前記第１および第2の判別結果に応じて、前記受信データの転送を実行する制御工程を実行するプログラムを格納したことを特徴とする記憶媒体。

【請求項１１】　第１のネットワークからの受信データを第2のネットワークへ転送する通信装置において、

前記受信データの転送先に対応する暗号情報を有しているかどうか判断する判断手段と、

前記判断に応じて、前記転送先に対応する暗号情報に基いて暗号化した受信データを前記転送先に転送する、あるいは、前記受信データを所定のメモリに格納するように制御する制御手段を有することを特徴とする通信装置。

【請求項１２】　請求項１１において、前記制御手段は前記受信データが所定のメモリに格納されたことを示すメッセージを前記転送先に送信することを特徴とする通信装置。

【請求項１３】　請求項１１において、前記暗号情報は前記転送先から取得することを特徴とする通信装置。

【請求項１４】　請求項１１において、前記制御手段は、前記受信データの機密度に応じて、前記暗号化を行うことを特徴とする通信装置。

【請求項１５】　請求項１１において、前記制御手段は、前記転送先から暗号情報を取得すると、前記所定のメモリに格納された受信データを前記暗号情報により暗号化した後、前記転送先に転送することを特徴とする通信装置。

【請求項１６】　請求項１１において、前記制御手段は前記転送先までの転送経路に応じて、前記暗号化を行うことを特徴とする通信装置。

【請求項１７】　請求項１１において、前記暗号情報は有効期限を含むことを特徴とする通信装置。

【請求項１８】　請求項１７において、前記暗号情報の有効期限は更新可能であることを特徴とする通信装置。

【請求項１９】　第１のネットワークからの受信データを第2のネットワークへ転送する通信方法において、

前記受信データの転送先に対応する暗号情報を有しているかどうか判断する判断工程と、

前記判断に応じて、前記転送先に対応する暗号情報に基いて暗号化した受信データを前記転送先に転送する、あるいは、前記受信データを所定のメモリに格納するように制御する制御工程を有することを特徴とする通信方法。

【請求項２０】　第１のネットワークからの受信データを第2のネットワークへ転送する通信方法のプログラムを格納したコンピュータ読取可能な記憶媒体において、

前記受信データの転送先に対応する暗号情報を有しているかどうか判断する判断工程と、

前記判断に応じて、前記転送先に対応する暗号情報に基いて暗号化した受信データを前記転送先に転送する、あるいは、前記受信データを所定のメモリに格納するように制御する制御工程を実行するプログラムを格納したことを特徴とする記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、受信した機密データを転送するのに好適な通信装置に関する。

【０００２】

【従来の技術】

近年のインターネットの爆発的な普及により、従来は公衆回線網を介してのみの通信を行っていたファクシミリ装置が、ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）等のコンピュータネットワークにも接続されるようになってきた。

【０００３】

このような公衆回線網とＬＡＮに接続可能なマルチ回線対応のファクシミリ装置は、ファクシミリ装置から公衆回線網を経由して画像データを受信すると、該画像データをＬＡＮ経由でサーバコンピュータに転送する。

【０００４】

ユーザは、クライアントコンピュータによりサーバコンピュータにアクセスして画像データを取得する。取得した画像データは所定のビュワーソフトによりＣＲＴ上に表示して閲覧することができる。あるいは、クライアントコンピュータに接続されるプリンタにより、画像データを印刷して閲覧することもできる。

【０００５】

ところで、ファクシミリ通信には、親展機能と呼ばれる機能が存在する。これはファクシミリ装置が親展送信の指定とともに受信した画像をすぐに印刷せずにメモリに格納しておき、所定のパスワード入力により該メモリから印刷するものである。これにより、親展番号のパスワードを知るユーザにしか画像を閲覧することができないようにしたものである。

【０００６】

【発明が解決しようとする課題】

しかしながら、上記従来例のファクシミリ装置では、親展画像を転送するための構成が無いため、親展文書の受取人であるユーザは、わざわざ当該ファクシミリ装置が設置してある場所まで出向いて、パスワードを入力することにより親展画像を印刷しなければならなかった。

【０００７】

【課題を解決するための手段】

本発明は、上記課題を解決するために、第１のネットワークからの受信データを第2のネットワークへ転送する通信装置において、前記受信データの転送先情報を判別する第１の判別手段と、前記受信データの機密度情報を判別する第2の判別手段と、前記第１および第2の判別結果に応じて、前記受信データの転送を実行する制御手段を有することを特徴とする通信装置を提供する。

【０００８】

また、本発明は、上記課題を解決するために、第１のネットワークからの受信データを第2のネットワークへ転送する通信装置において、前記受信データの転送先に対応する暗号情報を有しているかどうか判断する判断手段と、前記判断に応じて、前記転送先に対応する暗号情報に基いて暗号化した受信データを前記転送先に転送する、あるいは、前記受信データを所定のメモリに格納するように制御する制御手段を有することを特徴とする通信装置を提供する。

【０００９】

【発明の実施の形態】

以下、図面を参照しながら本発明に係る実施の形態を詳細に説明する。

【００１０】

図１は本発明の通信装置の構成を示したブロック図である。同図において１０１は装置全体の制御を司るＣＰＵ、１０２はＣＰＵ１０１が実行する制御プログラムが記憶されたＲＯＭ、１０３はデータの一時保存領域となるＲＡＭである。ここでＲＡＭの一部は電池等によりバックアップされた不揮発性メモリになっており、本実施形態で必要な登録データや管理テーブル等、装置の電源がオフしても保持しておくべきデータが格納されている。尚、該不揮発性メモリはハードディスク装置等が代替してもよい。

【００１１】

１０４は外部回路とのデータの入出力を行うＰＩＯ、１０５はＰＩＯ１０４によって制御される操作パネル、１０６はデータを圧縮する圧縮回路、１０７はデータの伸張を行う伸張回路、１０８はデジタルデータを公衆回線網２０２に送出するために音声帯域のアナログ信号に変換するための変調回路、１０９は公衆回線網２０２から受信したアナログ信号をデジタル信号に復調する復調回路、１１０は変調回路１０８と復調回路１０９とからなるＭＯＤＥＭ、１１１は本装置を公衆回線網２０２と接続するためのＮＣＵ、１１２は信号をＬＡＮへ送出するためのプロトコルに関する制御を司るＬＡＮコントローラ、１１３は信号レベルで本装置内の信号とＬＡＮ上の信号のマッチングを取るために利用されるＬＡＮ接続回路、１１４はＣＰＵ１０１が制御を行うために利用するＣＰＵバスである。

【００１２】

また図２は本発明の通信装置２０１が接続されるネットワークシステムを示した図である。同図より、通信装置２０１は公衆回線網２０２とＬＡＮ２０３にそれぞれ接続されている。ＬＡＮ２０３上には受信した画像データを保管する等の目的で利用されるサーバコンピュータ２０５、サーバコンピュータ２０５と情報交換が可能なクライアントコンピュータ２０６が接続されている。ここで、サーバコンピュータ２０５は、ＳＭＴＰサーバ機能やＰＯＰサーバ機能等の電子メールサーバ機能を備えており、通信装置２０１、クライアントコンピュータ２０６、並びにその他の不図示の端末との間で電子メールの交換が可能なように構成されている。ここで、通信装置２０１、および、クライアントコンピュータ２０６は、電子メールクライアント機能を備えていることは言うまでもない。

【００１３】

また、通信装置２０１は公衆回線網２０２を介してファクシミリ装置２０４とファクシミリ通信を実行する。

【００１４】

＜第１の実施形態＞

第１の実施形態は、通信装置２０１が公衆回線網２０２から受信した画像データをサーバコンピュータ２０５に送信して所定の領域に格納する構成において、受信した画像データが親展画像か否かに基づいて画像データの暗号化処理を選択的に実行するものである。

【００１５】

すなわち、受信した画像データが親展画像である場合には、所定の方式により暗号化して格納することにより、特定のユーザしか閲覧できないようにする。これにより受信した親展画像の機密性を維持したまま転送することが可能となる。

【００１６】

以下、図３のフローチャートを用いて、本実施形態の通信装置２０１の動作を説明する。まず、通信装置２０１は電源投入後プログラムが開始（ステップＳ３０１）され、公衆回線網２０２の着信待ち状態（ステップＳ３０２）に移行する。着信の待機中に、ファクシミリ２０４からの発信があると、その呼が公衆回線網２０２を経由して通信装置２０１へ届き着信する。ＣＰＵ１０１、ＮＣＵ１１

１によって当該着信を検知するとＮＣＵ１１１を用いて送信側と呼を確立する。

【００１７】

その後、ＩＴＵ－Ｔ勧告Ｔ．３０に準拠したフェーズＢの処理へと移行し、通信能力情報の交換や通信回線の品質を調査するトレーニングを行う（これを事前交信として表す）。事前交信（ステップＳ３０３）では、前述のサブアドレス（ＩＴＵ－Ｔ Ｔ．３０におけるＳＵＢ信号による）や、親展画像の場合にはパスワード（ＩＴＵ－Ｔ Ｔ．３０におけるＰＷＤ信号による）、親展ボックス番号等の情報の通知が行われる。これらの情報は通信装置２０１内のＲＡＭ１０３へ一時的に保存される。

【００１８】

事前交信（ステップＳ３０３）が終了すると、画像データの受信（ステップＳ３０４）が実行される。ここでは、公衆回線網２０２を介して送られてきた画像信号が、ＮＣＵ１１１から通信装置２０１内に取り込まれ、ＭＯＤＥＭ１１０の復調回路１０９を経て、伸張回路１０７によって元の画像データに戻された後、所定のデータ形式（圧縮データであってもよい）にしてＣＰＵ１０１によってＲＡＭ１０３に保存される。この受信動作は送信側から終了通知が届くまで繰り返し実行される（ステップＳ３０５）。

【００１９】

画像データの受信が終了すると、この画像が親展画像であるか否かを、前述したＲＡＭ１０３に保存された情報を読み出すことによって判断する（ステップＳ３０６）。尚、この判断では、上記のＰＷＤ信号を受信したか否かに基づいて判断してもよいし、ＮＳＳ信号等の手順信号上で、親展機能を利用する旨の指定がされているか否かに基づいて判断してもよい。

【００２０】

画像データが親展画像であった場合は、ＣＰＵ１０１によってＲＡＭ１０３へ保存した画像データを読み出した後、画像データの暗号化処理を行う（ステップＳ３０７）。ここで、通信装置２０１は、サーバコンピュータ２０５に対応する暗号鍵で暗号化を行う。

【００２１】

そして、この暗号化された画像データをＬＡＮコントローラ１１２に送り、ＬＡＮ接続回路１１３を介して、ＬＡＮ２０３上へと送出し、サーバコンピュータ２０５へと転送する（ステップＳ３０８）。またＣＰＵ１０１は事前交信（ステップＳ３０３）で得たパスワードと親展ボックス番号を併せてサーバコンピュータ２０５へ送信し、通信装置２０１は処理を終了する（ステップＳ４０９）。

【００２２】

ステップＳ３０６において、画像データが親展画像でなかった場合は、暗号化の処理であるステップＳ３０７はパスされ、画像データを暗号化せずにサーバコンピュータ２０５へと転送（ステップＳ３０８）し、通信装置２０１は処理を終了する（ステップＳ３０９）。

【００２３】

ここで、上記ステップＳ３０８で転送された画像データを受信したサーバコンピュータ２０５は、該画像データを自身の記憶領域にファイルとして保存し、サブアドレスを元に画像データの受信通知を特定のユーザのクライアントコンピュータ２０６へ送信する。この通知手段は例えば電子メールによって行われる。

【００２４】

画像データが親展画像でない場合には、この通知を受け取ったユーザは、クライアントコンピュータ２０６を操作し、サーバコンピュータ２０５から自分宛に届いた画像データをダウンロードするなどして入手し、画像ビュワアプリケーションを用いてクライアントコンピュータ２０６上に表示させたり、不図示のプリンタ装置を使って印刷させたりして画像データを可視情報として取得することが可能となる。

【００２５】

一方、画像データが親展画像であり、サーバコンピュータ２０５に保存された画像データが暗号化されている場合は、クライアントコンピュータ２０６がサーバコンピュータ２０５から画像データをダウンロードする際に親展ボックス番号に対応したパスワードをサーバコンピュータ２０５へ送信する必要がある。サーバコンピュータ２０５ではこのパスワードが正しい物であると判断した場合のみ、クライアントコンピュータ２０６へ復号化した画像データを送り、クライアン

トコンピュータ２０６を介して閲覧することが可能となる。

【００２６】

＜第２の実施形態＞

第２の実施形態は、通信装置２０１が公衆回線網２０２から受信した画像データをサーバコンピュータ２０５に送信して所定の領域に格納する構成において、受信した画像データが親展画像である場合には、該格納を行わずに指定された転送先に電子メールにより転送するものである。

【００２７】

これにより、受信した画像データが親展画像である場合には、サーバコンピュータ２０５上のメモリに格納されることなく直接転送先に電子メール転送されるので、受信した親展画像の機密性を維持したまま転送を実行することが可能となる。

【００２８】

以下、図４のフローチャートを用いて、本実施形態の通信装置２０１の動作を説明する。ここでステップＳ４０１～４０５の処理については、上記第１の実施形態のステップＳ３０１～３０５において説明しているので、ステップＳ４０６から説明する。

【００２９】

まず、ステップＳ４０５で受信した画像データが親展画像であるか否かを、前述したＲＡＭ１０３に保存された情報を読み出すことによって判別し（ステップＳ４０６）、親展画像の場合には、ＣＰＵ１０１によってＲＡＭ１０３へ保存した画像データを読み出した後、ＣＰＵ１０１は読み出した画像データをクライアントコンピュータ２０６によって展開が可能な画像フォーマット（JPEG,GIFなど）に変換する（ステップＳ４０７）。続いてＣＰＵ１０１はサブアドレスに基づいて転送先のクライアントコンピュータ２０６を特定し、電子メールを送信する（ステップＳ４０８）。その際、この電子メールに画像フォーマットに変換した画像データを添付して送ることにより、親展画像を特定のユーザに電子メールで届けることが実現する。画像フォーマットに変換した画像データを添付した電子メールの送信が終了すると、通信装置２０１は処理を終了する（ステップＳ４０

９）。

【００３０】

ステップＳ４０６において、受信した画像データが親展画像でない場合は、画像データをサーバコンピュータ２０５へと転送（ステップＳ４１０）し、通信装置２０１は処理を終了する（ステップＳ４０９）。サーバコンピュータ２０５は受け取った画像データを自身の記憶領域にファイルとして保存し、サブアドレスを元に画像データの受信通知を特定のユーザのクライアントコンピュータ２０６へ送信する（ステップＳ４１１）。この通知手段は例えば電子メールによって行われる。この通知を受け取ったユーザは、クライアントコンピュータ２０６を操作し、サーバコンピュータ２０５から自分宛に届いた画像データをダウンロードするなどして入手し、画像ビュワアプリケーションを用いてクライアントコンピュータ２０６上に表示させたり、図示していないがプリンタ装置を使って印刷するなどして画像データを閲覧することが可能である。

【００３１】

＜第3の実施形態＞

第3の実施形態として、受信した親展画像を電子メールで転送する際に、転送先の公開鍵を取得しているか否かに基づいて暗号化を選択的に実行する例を示す。

【００３２】

すなわち、通信装置２０１が、親展画像の転送先の公開鍵を取得している場合には、受信した画像データを該公開鍵により暗号化した電子メールにより転送する。通信装置２０１が、親展画像の転送先の公開鍵を取得していない場合には、該親展画像は転送せずに、通信装置２０１が管理するメモリボックスに格納しておき、転送先には、受信した親展画像をメモリボックスに格納した旨を記載した電子メールのみを送信する。

【００３３】

ここで、公開鍵方式は、送信側の暗号化鍵と受信側の復号化鍵とが異なった暗号鍵であり、一方（公開鍵）を公開し、他方（秘密鍵）を秘密にするものであるので、自分の公開鍵で暗号化された親展画像を受信したユーザは、自分のみが所

有する秘密鍵を用いて復号化して親展画像を閲覧すればよい。

【００３４】

これにより、親展画像が暗号化されずに、不用意にＬＡＮ上に流出してしまうのを防止し、親展画像の機密性を維持することが可能となる。

【００３５】

図６は、通信装置２０１が有するサブアドレスデータと転送先の電子メールアドレスとの対応を記憶した管理テーブルである。このテーブルには、サブアドレスデータ６０１に対する転送先の電子メールアドレスと親展ボックス番号とが対応づけられて記憶されている。

【００３６】

また、図７は、通信装置２０１の電子メールクライアント機能が有するアドレス帳のデータ構造をテーブルとして示した図である。同図より、宛先ごとに宛先名７０１、電子メールアドレス７０２、該宛先の公開鍵を所有しているか否かの情報７０３とが対応づけられている。尚、公開鍵データは、予めそれぞれの宛先からＬＡＮ経由で取得するか、若しくは、通信装置２０１に着脱可能な記憶媒体をドライブする装置を接続する機能を具備させて、該記憶媒体を介して取得する。取得した公開鍵データはファイルデータとして格納しておき、所定操作によりアドレス帳に取得した公開鍵と宛先と対応づけておく。

【００３７】

また、公開鍵を取得する際に、所定の認証機関により当該公開鍵が本人のものであることを証明する証明書を合わせて受け取り、該公開鍵の正当性を確認した後、公開鍵を上記アドレス帳に登録する手順をとると好適である。

【００３８】

では、図６および図７を用いて、本実施形態を説明する。

【００３９】

まず、公衆回線網２０２からサブアドレス「０１２３」が指定された画像データを受信すると、図６の管理テーブルから転送先の電子メールアドレスは「ａａａ＠×××．×××．ｃｏｍ」と変換され、さらに図７のアドレス帳から転送先の電子メールアドレスをキーとして公開鍵の有無が判別される。

【００４０】

したがって、図６および図７の例によれば、サブアドレス「０１２３」および「８９０１」が指定された親展画像については、公開鍵を所有していないので、それぞれ、対応するメモリボックス「０１」および「０３」に格納され、格納した親展ボックス番号や、送信元情報、受信日時をテキストデータとして記載した電子メールをそれぞれの転送先である「ａａａ@×××．×××．ｃｏｍ」および「ｃｃｃ@×××．×××．ｃｏｍ」に転送する。

【００４１】

サブアドレス「４５６７」が指定された親展画像については、公開鍵を所有しているので、その公開鍵により親展画像を暗号化して、転送先である「ｂｂｂ@×××．×××．ｃｏｍ」に転送する。

【００４２】

また、受信した画像データが親展画像でない場合には、サブアドレスに対応した転送先の電子メールアドレスに対して、受信した画像データを暗号化せずに電子メールで転送する。

【００４３】

図５は、本実施形態における通信装置２０１の動作を示すフローチャートである。ここでステップＳ５０１～５０５の処理については、上記第１の実施形態のステップＳ３０１～３０５において説明しているので、ステップＳ５０６から説明する。

【００４４】

まずステップＳ５０６において、ステップＳ５０４で受信した画像データが親展画像であるか否かを判別し、親展画像でない場合にはステップＳ５１２に進み、ステップＳ５０３で受信したサブアドレスに対応する転送先の電子メールアドレスに該受信した画像データを添付した電子メールを送信する。

【００４５】

ステップＳ５０７では、ステップＳ５０３で受信したサブアドレスに対応する電子メールアドレスに公開鍵が関連づけられているか否かを上記図６の管理テーブルおよび図７のアドレス帳に基づいて判断する。公開鍵が関連づけられていな

い場合には、ステップＳ５１０に進み、受信した画像データをサブアドレスに対応するメモリボックスに格納する。そしてステップＳ５１１で、サブアドレスに対応する電子メールアドレスに対して、親展画像をメモリボックスに格納した旨のメッセージを本文データとして記載した電子メールを送信する。該メッセージの例として、「あなたのメモリボックスに親展画像を受信しましたので受け取りに来てください」等を用いればよい。

【００４６】

ここで、該メッセージを記載した電子メールを受信した親展画像の受取人が、通信装置２０１の設置場所まで出向き、上記メモリボックスに対応するパスワードを操作パネル１０５から入力することにより、親展画像が不図示のプリンタから出力される。これにより、親展画像が暗号化されないまま不用意にＬＡＮ上に送出されることがなくなり親展画像の機密性を維持することが可能となる。

【００４７】

ステップＳ５０７の判断で、公開鍵が関連づけられている場合には、ステップＳ５０８に進み、受信した画像データを該公開鍵で暗号化し、ステップＳ５０９で該暗号化した親展画像を添付した電子メールにより転送する。公開鍵による暗号化方式としては、例えばＲＳＡ（Rivest-Shamir-Adleman ）方式等がある。

【００４８】

以上の処理により、公衆回線網から受信した親展画像をＬＡＮ経由で転送する際に、確実に暗号化して転送することが可能となり、親展画像の機密性が維持される。

【００４９】

尚、暗号方式には上記の公開鍵方式の他に共通鍵方式がある。共通鍵方式は、送信側の暗号化鍵と受信側の復号化鍵とが同じ暗号鍵であり、その暗号鍵によって送信側で通信文（平文）を暗号化して送信し、受信側で受け取った通信文（暗号文）を同じ暗号鍵で復号化するものである。

【００５０】

一般に公開鍵方式は、共通鍵方式にくらべて、暗号化とその解読の処理が複雑で時間がかかる傾向があるので、所定のアルゴリズムにより生成した共通鍵によ

り親展画像を暗号化したデータと、該共通鍵を転送先の公開鍵で暗号化したデータとを転送するようにしてもよい。共通鍵による暗号化方式としてはＤＥＳ（Data Encryption Standard）方式等がある。

【００５１】

＜第４の実施形態＞

上記第３の実施形態では、上記ステップＳ５１０において、メモリボックスに格納した親展画像の受取人は、通信装置２０１に出向いてプリント出力するものとして説明したが、本実施形態では、親展画像をメモリボックスに格納した後、該親展画像の転送先の公開鍵が上記アドレス帳に登録されたことを契機として、自動的に該親展画像を該公開鍵で暗号化して転送先に転送するものである。

【００５２】

これにより、親展画像の受取人がわざわざ通信装置２０１まで出向かなくても、管理者等に公開鍵を登録してもらうか、ＬＡＮ２０３経由で公開鍵を通信装置２０１に送れば、メモリボックス内の親展画像を取得することが可能となる。

【００５３】

本実施形態における通信装置２０１の動作を図９のフローチャートを参照して説明する。尚、図９のフローチャートは第３実施形態のフローチャートをモディファイしたものであり、同一符号のステップについては、同一の処理であることを示している。以下、処理の異なるステップについて説明する。

【００５４】

まず、図１０のステップＳ５１１の処理後、メモリボックスに格納した親展画像に対応する宛先の公開鍵がアドレス帳に登録されたか否かを判定する判定プロセスを所定周期で実行し（ステップＳ１００１、ステップＳ１００２のループ処理）、ステップＳ１００１において、該判定プロセスの肯定判定を検出したら、ステップＳ５０８に進み、登録された公開鍵により親展画像を暗号化して転送を行う。

【００５５】

また、ステップＳ５１１で送信するメッセージとして、「あなたのメモリボックスに親展画像を受信しましたので、あなたの公開鍵をお送りいただければ暗号

化して送信します。」等を用いればよい。

【００５６】

＜第５の実施形態＞

上記第３の実施形態では、転送先の公開鍵を保持していない場合には一律に転送を実行しないようにしたが、本実施形態は、転送経路のセキュリティに応じて暗号化転送を実行するものである。すなわち、ＬＡＮ２０３経由の転送において、転送経路のセキュリティが確保されていない場合に限って、転送先の公開鍵の有無を判断し、該判断の結果、公開鍵が有れば親展画像を暗号化して転送し、公開鍵が無ければ親展画像をメモリボックスに格納してその旨のメッセージのみを転送先に送信する。また、転送経路のセキュリティが確保されている場合には、転送先の公開鍵の有無にかかわらず、親展画像を転送先に転送する。

【００５７】

これにより、イントラネット等のセキュリティが確保されているドメイン内の転送先に対しては、公開鍵データのやりとりが不要となり、通信装置２０１の登録データを管理する手間を軽減することができる。

【００５８】

本実施形態における通信装置２０１の動作を図１０のフローチャートを参照して説明する。尚、図１０のフローチャートは上記第３実施形態の図５のフローチャート図をモディファイしたものであり、同一符号のステップについては、同一の処理であることを示している。以下、処理の異なるステップについて説明する。

【００５９】

まず、ステップＳ５０６において受信した画像データが親展画像であると判断されるとステップＳ１１０１に進む。ステップＳ１１０１ではステップＳ５０３で受信したサブアドレスに対応した転送先の転送経路のセキュリティを判断し、転送経路にセキュリティ有りと判断した場合には、ステップＳ５１２に進み親展画像を該転送先に転送する。

【００６０】

また、転送経路にセキュリティ無しと判断した場合にはステップＳ５０７に進

み、公開鍵の有無に基づいて親展画像を転送するかメモリボックスに格納するかを決定する。ここでステップＳ１１０１における転送経路のセキュリティの有無の判断は、例えば通信装置２１０の電子メールアドレスのドメインと転送先の電子メールアドレスのドメインに基づいて判断すればよい。

【００６１】

その判断を、図６および図７を参照して説明する。前に述べたように通信装置２０１の電子メールクライアント機能を備えており、その電子メールアカウントを「ｆａｘ@×××．×××．ｃｏｍ」とする。

【００６２】

したがって、図７のアドレス帳データの例によれば、宛先ａａａ、ｂｂｂ、及び、ｃｃｃが通信装置２０１と同一ドメイン「×××．×××．ｃｏｍ」内にあり、宛先ｄｄｄ、及び、ｅｅｅが通信装置２０１とは異なるドメインにあることがわかる。

【００６３】

そこで、通信装置２０１と同一のドメイン内の転送先については、アドレス帳に公開鍵が登録されているか否かにかかわらず、親展画像を添付した電子メールにより転送を行う。

【００６４】

通信装置２０１と異なるドメイン内の転送先については、アドレス帳に公開鍵が登録されているか否かに応じた方式により転送を行う。すなわち、宛先ｄｄｄは公開鍵が登録されていないので、ｄｄｄ宛ての親展画像は対応するメモリボックス０４に格納し、宛先ｄｄｄに対してはメモリボックス０４に親展画像を格納したメッセージを本文に記載した電子メールのみを送信する。また、宛先ｅｅｅに対しては、公開鍵が登録されているので、該公開鍵により暗号化した親展画像を添付した電子メールをｅｅｅ宛てに送信する。

【００６５】

尚、ドメイン名はドット（ｄｏｔ）で区切った階層構造になっていおり、第１階層である「ｃｏｍ」を起点としてどの層までの一致をもって同一ドメインと判断するかは、ネットワークシステムのセキュリティポリシーに基づくので、例え

ば、「×××．ｃｏｍ」の第２階層までの一致をもって転送経路のセキュリティ有りと判断してもよい。

【００６６】

また、上記の例はドメイン名に基づいた判断であるが、転送先のＩＰアドレスのサブネットが所定のサブネットの範囲内にあるか否かに基づいてセキュリティの有無を判断してもよい。

【００６７】

＜第６の実施形態＞

公開鍵には、機密性を高めるために期限付きで有効になるものがある。本実施形態では、このような公開鍵を利用する場合について図１１を参照して説明する。

【００６８】

尚、図１１のフローチャートは上記第３実施形態の図５のフローチャート図をモディファイしたものであり、同一符号のステップについては、同一の処理であることを示している。以下、処理の異なるステップについて説明する。

【００６９】

まず、ステップＳ５０６において受信した画像データが親展画像であると判断されると、ステップS５０７において、ステップＳ５０３で受信したサブアドレスに対応する電子メールアドレスに公開鍵が関連づけられているか否かを上記図６の管理テーブルおよび図７のアドレス帳に基づいて判断する。

【００７０】

ステップS５０７で公開鍵が関連づけられていると判断された場合は、ステップＳ１２０１において、その公開鍵が有効期限内かどうか判定する。

【００７１】

ステップＳ１２０１で公開鍵が有効期限内であれば、ステップＳ５０８において、受信した画像データを該公開鍵で暗号化する。そして、ステップＳ５０９において、該暗号化した親展画像を添付した電子メールにより転送する。

【００７２】

ステップＳ１２０１において、公開鍵が有効期限切れであれば、ステップＳ５

１０において、受信した画像データをサブアドレスに対応するメモリボックスに格納する。そして、ステップＳ５１１において、サブアドレスに対応する電子メールアドレスに対して、親展画像をメモリボックスに格納した旨のメッセージを本文データとして記載した電子メールを送信する。該メッセージの例として、「公開鍵の有効期限が切れています。あなたのメモリボックスに親展画像を受信しましたので受け取りに来てください」等を用いればよい。

【００７３】

また、公開鍵の有効期限が更新されたことを契機として、自動的に該親展画像を該公開鍵で暗号化して転送先に転送するようにしてもよい。

【００７４】

この場合の通信装置２０１の動作を図１２のフローチャートを参照して説明する。尚、図１２のフローチャートは第３実施形態のフローチャートをモディファイしたものであり、同一符号のステップについては、同一の処理であることを示している。以下、処理の異なるステップについて説明する。

【００７５】

まず、図１２のステップＳ５１１の処理後、ステップＳ１３０４において、メモリボックスに格納した親展画像に対応する宛先の公開鍵の有効期限が更新されたか否かを判定する判定プロセスを所定周期で実行し（ステップＳ１３０２、ステップＳ１３０３のループ処理）、ステップＳ１３０２において、該判定プロセスの肯定判定を検出したら、ステップＳ１３０１に進み、更新された期限が有効か否かを判定する。

【００７６】

ステップＳ１３０１で公開鍵が有効期限内であると判定されれば、ステップＳ５０８において、受信した画像データを該公開鍵で暗号化する。そして、ステップＳ５０９において、該暗号化した親展画像を添付した電子メールにより転送する。

【００７７】

また、ステップＳ５１１で送信するメッセージとして、「公開鍵の有効期限が切れています。あなたのメモリボックスに親展画像を受信しましたので、あなた

の公開鍵の有効期限更新手続をしていただければ暗号化して送信します。」等を用いればよい。

【００７８】

尚、本実施の形態では、公開鍵の有効期限を更新する場合について述べたが、転送先から新たに有効期限内にある公開鍵を取得したことを契機として、所定のメモリボックスに格納された親展画像を暗号化して転送するようにしても良い。

【００７９】

＜第７の実施形態＞

上記実施形態では、通信装置という１つの機器を用いた動作により説明したが、パーソナルコンピュータ及びモデム、スキャナ、プリンタ等の複数の機器から構成されるシステムに本発明を適用してもよい。図８を用いてそのシステム構成を簡単に説明する。同図より、パーソナルコンピュータ８０２（以下、ＰＣ８０２と称する）に、スキャナ８０１、プリンタ８０３、モデム８０４（ＰＣ８０２に内蔵されていてもよい）が、所定のインターフェースを介して接続されている。また、ＰＣ８０２は、モデム８０４を介して公衆回線網２０２に接続され、不図示のＬＡＮボードを介してＬＡＮ２０３に接続されている。

【００８０】

尚、ＰＣ８０２と、スキャナ８０１、および、プリンタ８０３、および、モデム８０４との接続インターフェースは、ＬＡＮ２０３を介したネットワークインターフェースであってもよいが、親展画像等の秘匿データを扱う関係上、ＵＳＢ等のＬＡＮ２０３と分離されたローカルインターフェースが好適である。

【００８１】

このシステムでの受信動作について説明すると、まず、公衆回線網２０２から送られてきた信号はモデム８０５に内蔵されたＮＣＵ部を介してモデム８０５へ取り込まれる。モデム８０５ではこのアナログ信号を復調して、デジタルデータを復元する。このデジタルデータはコンピュータ８０７から読み出され、圧縮データの解凍により画像データを復元したのち、プリンタ８０８へ送られる。プリンタ８０８ではこの画像データを印刷する。

【００８２】

このとき受信した画像データが親展であれば、ＰＣ８０２が内蔵するハードディスク装置内のメモリボックスに格納され、上記第3実施形態によれば、公開鍵データを有する宛先に対しては該公開鍵により暗号化して親展画像を転送し、公開鍵データを有しない宛先に対しては親展画像を受信した旨を記述した電子メールを送信する。

【００８３】

以上、第１～７の実施形態について説明したが、これらの実施形態では、送信機から受信したサブアドレスを本発明に係る通信装置が電子メールアドレスに変換する例を示したが、送信機からのサブアドレス内に転送先の電子メールアドレスが直接セットされている形態であってもよい。

【００８４】

また、上記実施形態では、公衆回線網２０２からの受信した画像データをＬＡＮ２０３上のクライアント装置に宛てに転送する例を用いて説明したが、これに限定されるものではなく、ＬＡＮ２０３が所定のアクセスポイントを介してインターネットに接続された構成において、公衆回線網２０２からの受信した画像データをインターネット経由で転送してもよい。インターネットを経由した通信についてはそのセキュリティが重要視されており、本発明は好適である。

【００８５】

尚、公衆回線網からの受信した画像データを、該公衆回線網からインターネットのアクセスポイントへダイアルアップ接続して転送する場合にも、本発明は適用される。

【００８６】

また、本発明はシステム或は装置にプログラムを供給することによって達成される場合にも適用できることは言うまでもない。その場合、記憶媒体に格納された本発明を達成するためプログラムコードを該システム或は装置のコンピュータ（ＣＰＵもしくはＭＰＵ）が読み出し実行することによって、本発明の目的が達成される。

【００８７】

また、本発明は、コンピュータが読み出したプログラムコードを実行する際に

、コンピュータ上で稼動しているＯＳ（オペレーティングシステム）などが処理の一部を行うような場合も含むことは言うまでもない。

【００８８】

【発明の効果】

以上説明したように、本出願の発明によれば、公衆回線網から受信した親展画像を暗号化してＬＡＮ上のサーバコンピュータに保存することにより、特定のクライアント以外のユーザが、容易に親展画像を閲覧できないようになり、機密性を維持したまま親展画像をＬＡＮ上のクライアントに配信することが可能となる。

【００８９】

また、本出願の発明によれば、受信した親展画像を電子メールに添付して該画像の受取人であるユーザへ送信するようにしたので、該ユーザは、通信装置までわざわざ出向いて親展画像を印刷するような手間が無くなり、ユーザの操作負荷が著しく軽減される。

【００９０】

また、本出願の発明によれば、転送先の暗号鍵を保持している場合には、該暗号鍵により暗号化して転送し、保持していない場合には、所定のメモリボックスに格納するようにしたので、親展画像が暗号化されずに、不用意にＬＡＮ上に流出してしまうのを防止することができる。

【００９１】

また、本出願の発明によれば、親展画像をメモリボックスに格納した後、該親展画像の転送先の暗号鍵が登録されたことを検出したら自動的に該親展画像を該公開鍵で暗号化して転送先に転送するようにしたので、ユーザが親展画像を受け取るためわざわざ装置まで出向く必要がなくなる。

【００９２】

また、本出願の発明によれば、転送経路のセキュリティに基づいて暗号化転送を実行するようにしたので、セキュリティの確保されたネットワーク内での転送に際しては、暗号鍵のやりとりの手間がなくなり、装置管理者の負荷を軽減することが可能となる。

【００９３】

また、本出願の発明によれば、転送先の暗号鍵が有効期限内であれば、該暗号鍵により暗号化して転送するようにしたので、信頼性の高い暗号鍵により暗号化された親展画像を転送することができる。

【図面の簡単な説明】

【図１】

本発明の第１実施形態における通信装置の構成を示した図

【図２】

本発明の第１実施形態におけるネットワークシステムを示した図

【図３】

本発明の第１実施形態における通信装置の動作を示すフローチャート

【図４】

本発明の第２実施形態における通信装置の動作を示すフローチャート

【図５】

本発明の第３実施形態における通信装置の動作を示すフローチャート

【図６】

本発明の第３実施形態におけるサブアドレスと電子メールアドレスの対応を示した管理テーブルのデータ構造を示した図

【図７】

本発明の第３実施形態におけるアドレス帳のデータ構造を示した図

【図８】

本発明の第７実施形態における通信装置システムの構成を示した図

【図９】

本発明の第４実施形態における通信装置の動作を示すフローチャート

【図１０】

本発明の第５実施形態における通信装置の動作を示すフローチャート

【図１１】

本発明の第６実施形態における通信装置の動作を示すフローチャート

【図１２】

本発明の第６実施形態における通信装置の動作を示すフローチャート

【符号の説明】

２０１　通信装置

２０２　公衆回線網

２０３　ＬＡＮ

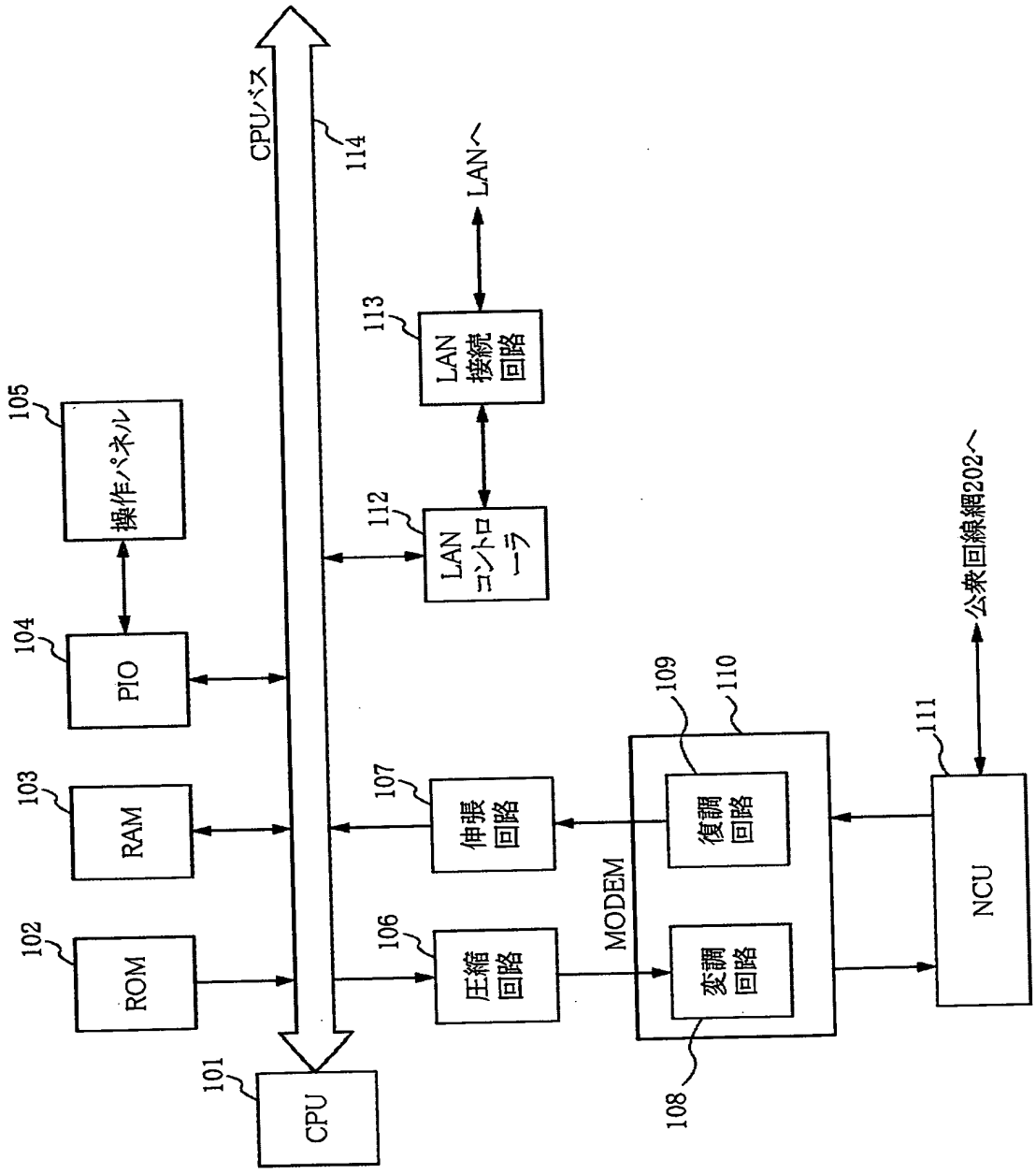
２０４　ファクシミリ装置

２０５　サーバコンピュータ

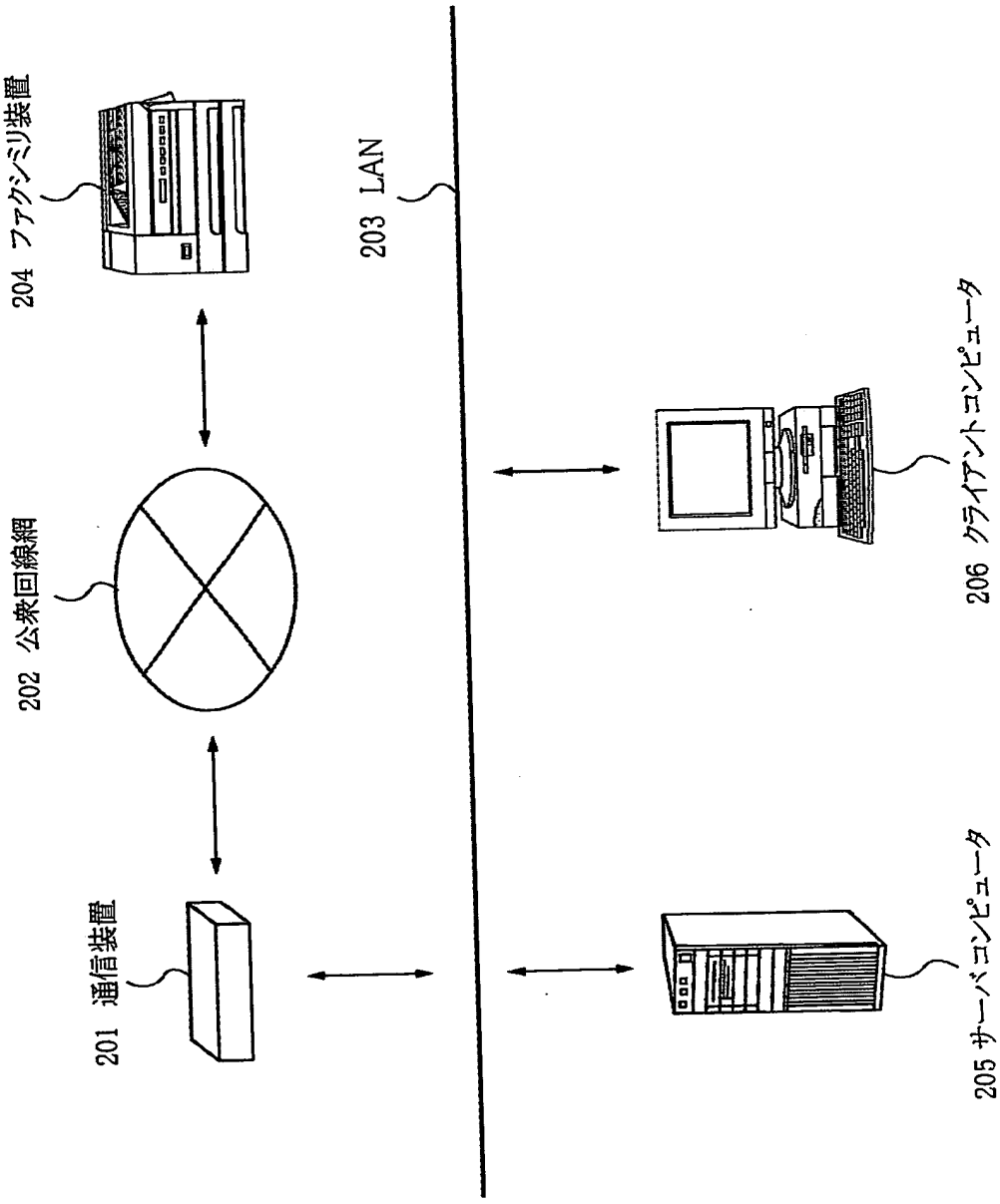
２０６　クライアントコンピュータ

【書類名】　図面

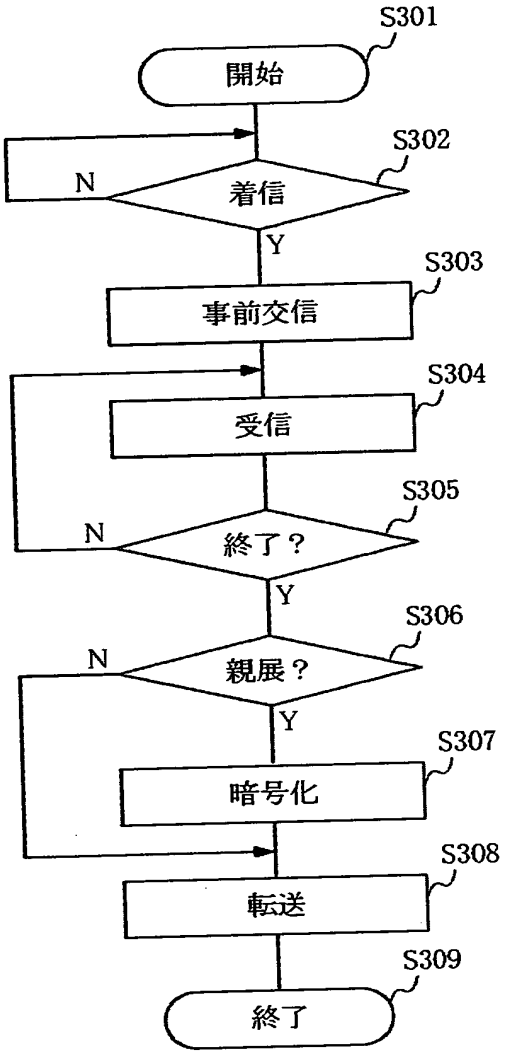
【図１】


CPUバス
114
LANへ
113
LAN
接続
回路
105
操作パネル
112
LAN
コントロ
ーラ
公衆回線網202へ
104
PIO
109
110
111
103
RAM
107
伸張
回路
復調
回路
MODEM
NCU
102
ROM
106
圧縮
回路
変調
回路
101
CPU
108

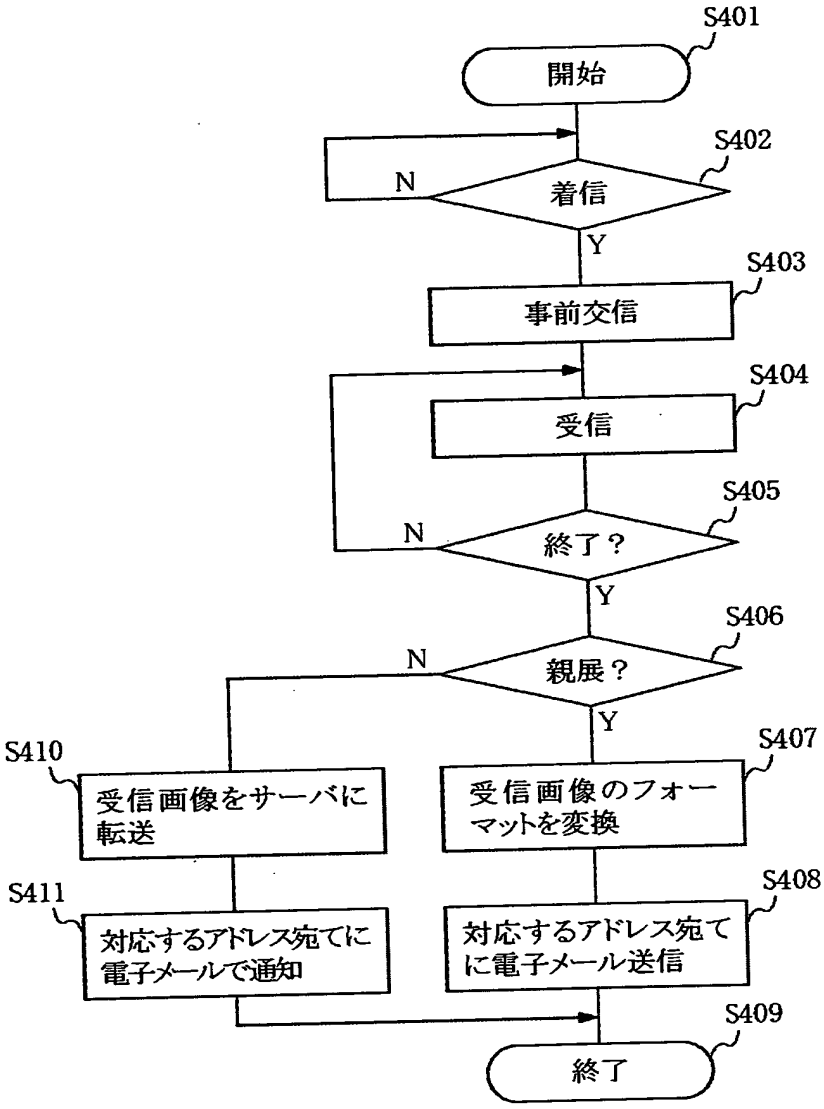
【図２】


204 ファクシミリ装置
203 LAN
202 公衆回線網
206 クライアントコンピュータ
201 通信装置
205 サーバコンピュータ

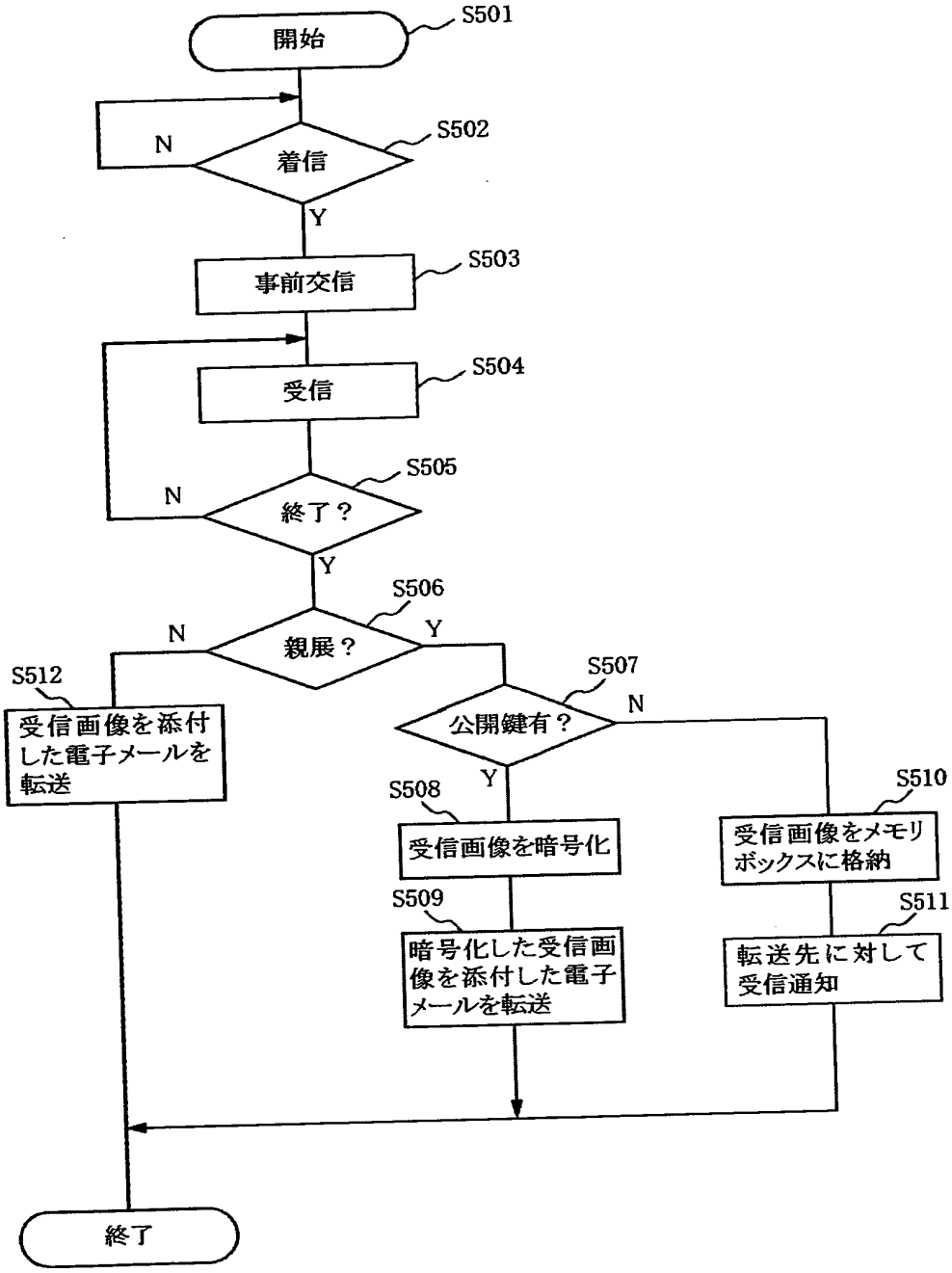
【図３】


S301
開始
S302
N
着信
Y
S303
事前交信
S304
受信
S305
N
終了？
Y
S306
N
親展？
Y
S307
暗号化
S308
転送
S309
終了

【図４】


S401
開始
S402
着信
N
Y
S403
事前交信
S404
受信
S405
終了？
N
Y
S406
親展？
N
Y
S407
受信画像のフォーマットを変換
S408
対応するアドレス宛てに電子メール送信
S410
受信画像をサーバに転送
S411
対応するアドレス宛てに電子メールで通知
S409
終了

【図５】


開始
S501
着信
S502
N
Y
事前交信
S503
受信
S504
終了？
S505
N
Y
親展？
S506
N
Y
S512
受信画像を添付した電子メールを転送
公開鍵有？
S507
N
Y
S508
受信画像を暗号化
S509
暗号化した受信画像を添付した電子メールを転送
S510
受信画像をメモリボックスに格納
S511
転送先に対して受信通知
終了

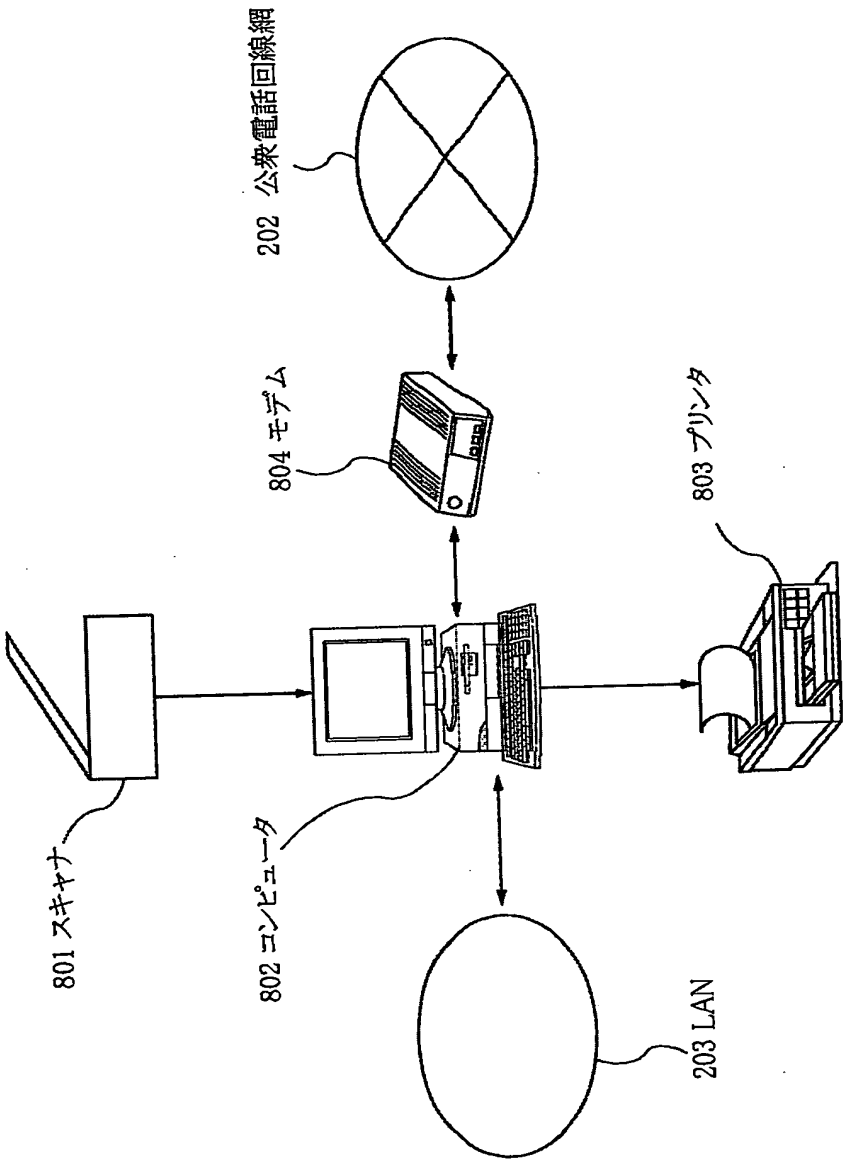
【図６】

| 601 サブアドレス | 602 転送先の電子メールアドレス | 603 メモリボックス |
|---|---|---|
| 0123 | aaa@canon. canon. com | 01 |
| 4567 | bbb@canon. canon. com | 02 |
| 8901 | ccc@canon. canon. com | 03 |
| 2345 | ddd@canon2. canon. com | 04 |
| 6789 | eee@canon2. canon. com | 05 |

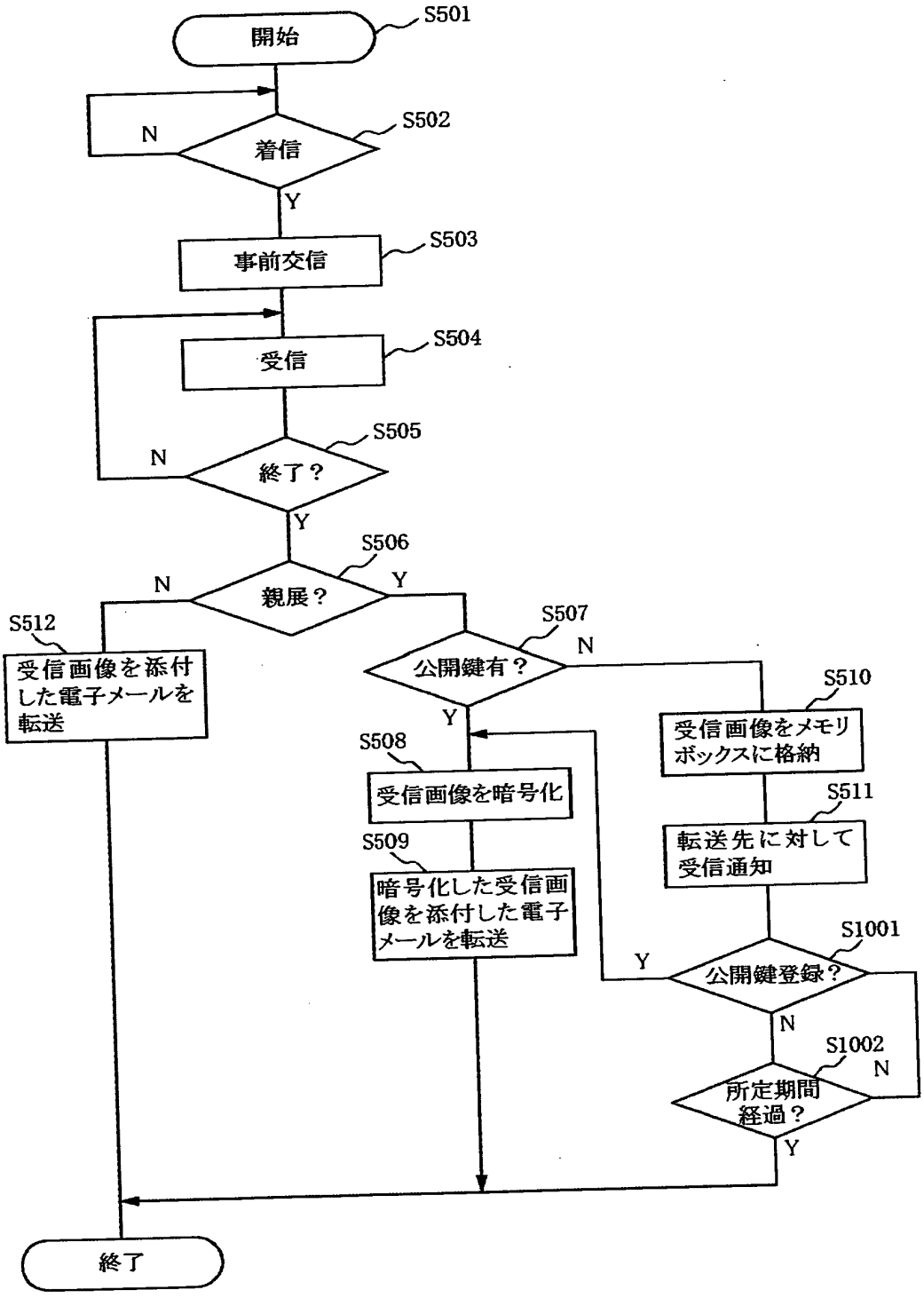
【図７】

| 701 宛先名 | 702 電子メールアドレス | 703 公開鍵 |
|---|---|---|
| aaa | aaa@canon. canon. com | 無し |
| bbb | bbb@canon. canon. com | 公開鍵bbb |
| ccc | ccc@canon. canon. com | 無し |
| ddd | ddd@canon2. canon. com | 無し |
| eee | eee@canon2. canon. com | 公開鍵eee |

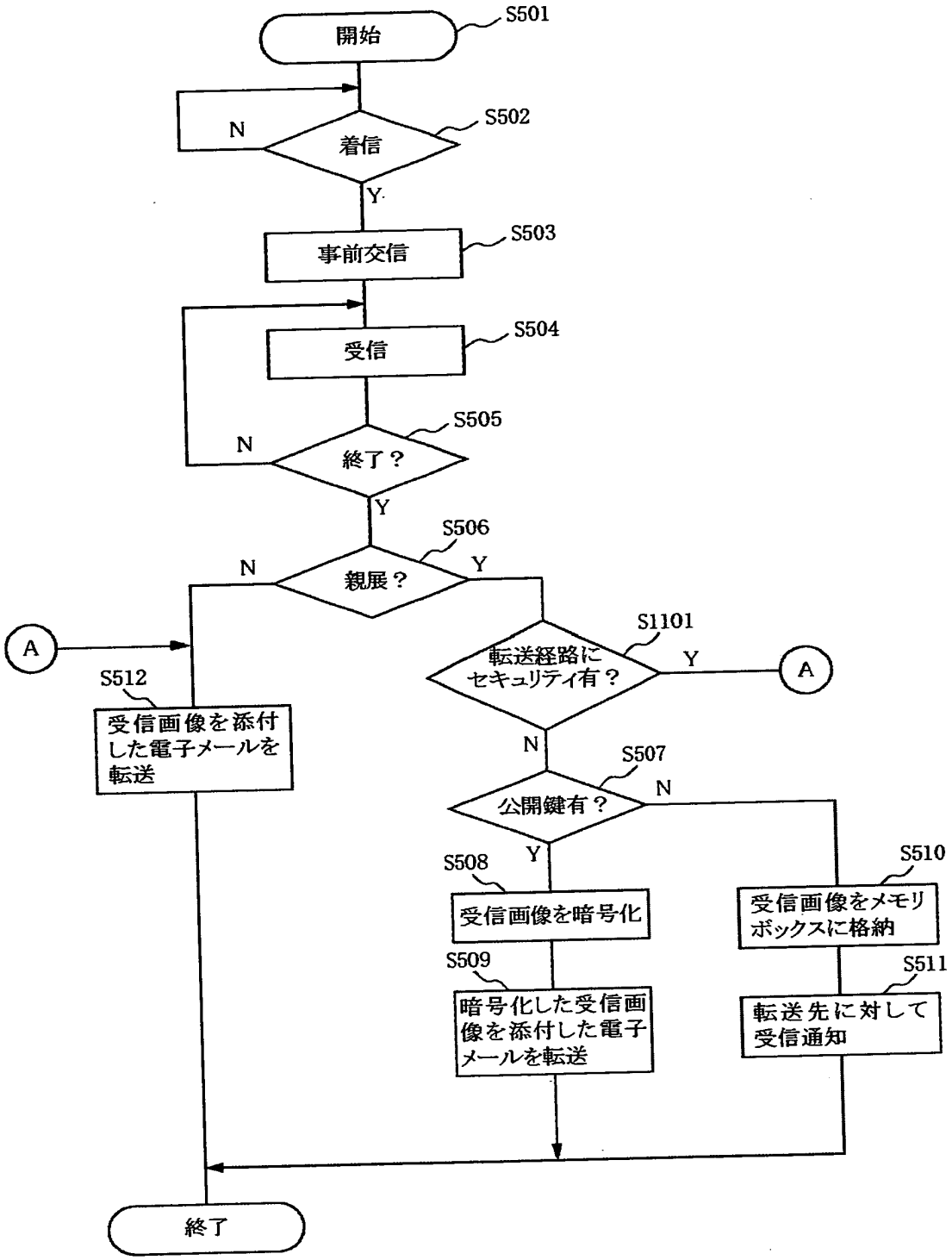
【図８】



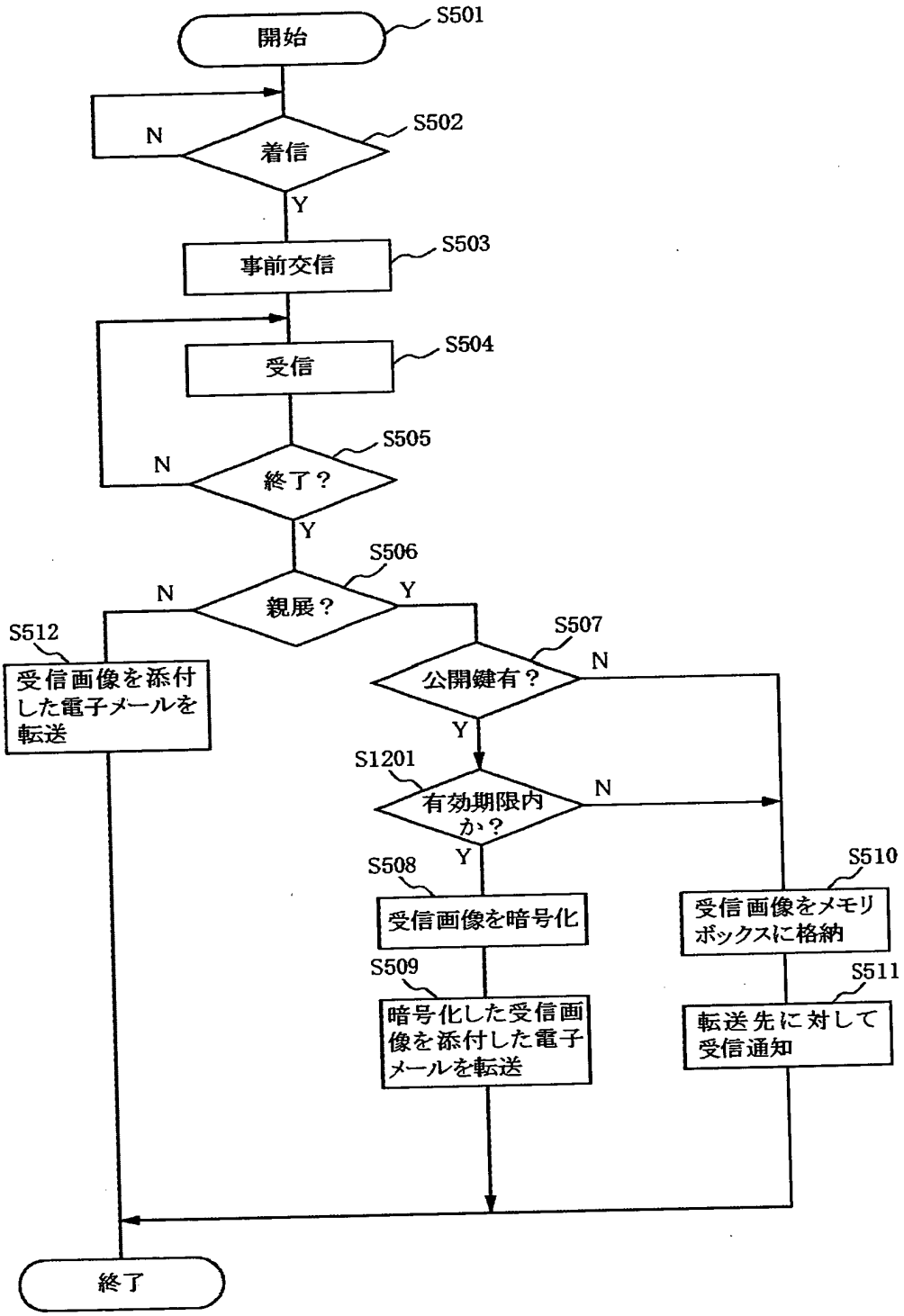
【図９】


開始
S501
着信
S502
N
Y
事前交信
S503
受信
S504
終了？
S505
N
Y
親展？
S506
N
Y
S512
受信画像を添付した電子メールを転送
公開鍵有？
S507
N
Y
S508
受信画像を暗号化
S509
暗号化した受信画像を添付した電子メールを転送
S510
受信画像をメモリボックスに格納
S511
転送先に対して受信通知
S1001
公開鍵登録？
Y
N
S1002
所定期間経過？
N
Y
終了

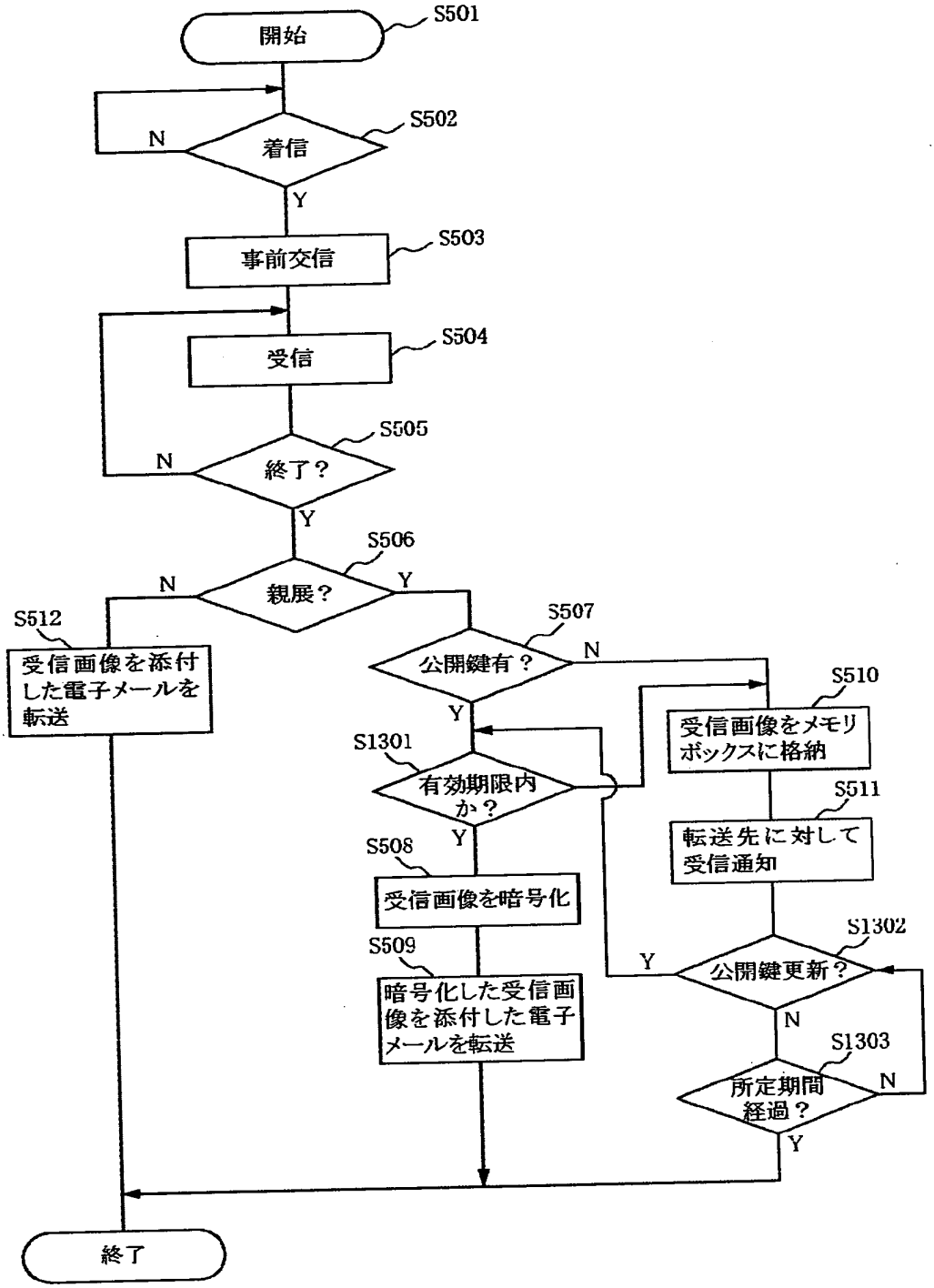
【図１０】


開始
S501
着信
S502
N
Y
事前交信
S503
受信
S504
終了？
S505
N
Y
親展？
S506
N
Y
A
S512
受信画像を添付した電子メールを転送
転送経路にセキュリティ有？
S1101
Y
A
N
公開鍵有？
S507
N
Y
S508
受信画像を暗号化
S509
暗号化した受信画像を添付した電子メールを転送
S510
受信画像をメモリボックスに格納
S511
転送先に対して受信通知
終了

【図１１】


開始
S501
着信
S502
N
Y
事前交信
S503
受信
S504
終了？
S505
N
Y
親展？
S506
N
Y
S512
受信画像を添付した電子メールを転送
公開鍵有？
S507
N
Y
S1201
有効期限内か？
N
Y
S508
受信画像を暗号化
S509
暗号化した受信画像を添付した電子メールを転送
S510
受信画像をメモリボックスに格納
S511
転送先に対して受信通知
終了

【図１２】


開始
S501
着信
S502
N
Y
事前交信
S503
受信
S504
終了？
S505
N
Y
親展？
S506
N
Y
S512
受信画像を添付した電子メールを転送
公開鍵有？
S507
N
Y
S1301
有効期限内か？
Y
S508
受信画像を暗号化
S509
暗号化した受信画像を添付した電子メールを転送
S510
受信画像をメモリボックスに格納
S511
転送先に対して受信通知
S1302
公開鍵更新？
Y
N
S1303
所定期間経過？
N
Y
終了

【書類名】　　要約書

【要約】

【課題】　受信した親展画像をその機密性を維持したまま所定の宛先に転送することが可能な通信装置及び方法並びに記憶媒体を提供することを目的とする。

【解決手段】　第１のネットワークからの受信データを第2のネットワークへ転送する通信装置において、前記受信データの転送先情報と機密度情報をそれぞれ判別し、それらの判別結果に応じて、前記受信データの転送を実行する。

【選択図】　　図２



出証特２０００－３１０２６７９

# 認定・付加情報

| | |
|---|---|
| 特許出願の番号 | 特願２０００－３２３９８０ |
| 受付番号 | ５００１３７３０２１ |
| 書類名 | 特許願 |
| 担当官 | 第八担当上席　　００９７ |
| 作成日 | 平成１２年１０月２７日 |

＜認定情報・付加情報＞

【特許出願人】

| | |
|---|---|
| 【識別番号】 | 000001007 |
| 【住所又は居所】 | 東京都大田区下丸子３丁目３０番２号 |
| 【氏名又は名称】 | キヤノン株式会社 |

【代理人】　申請人

| | |
|---|---|
| 【識別番号】 | 100090538 |
| 【住所又は居所】 | 東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内 |
| 【氏名又は名称】 | 西山　恵三 |

【選任した代理人】

| | |
|---|---|
| 【識別番号】 | 100096965 |
| 【住所又は居所】 | 東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内 |
| 【氏名又は名称】 | 内尾　裕一 |

次頁無

# 出願人履歴情報

識別番号　〔０００００１００７〕

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都大田区下丸子３丁目３０番２号
氏　名　キヤノン株式会社